APPARATUS, SYSTEM, AND METHOD FOR SEALING A DATA REPOSITORY TO A TRUSTED COMPUTING PLATFORM

ABSTRACT OF THE DISCLOSURE

An apparatus, method, and system to seal a data repository to a trusted computing platform is described. The data repository may be sealed by encrypting the data on the repository and sealing a cryptographic key to a specific set of platform resources. With the data repository sealed to the platform, the system boot sequence will fail if the system configuration is compromised, for example by insertion of "snoopware" or a modified BIOS. Additionally, if the computer containing the data repository is lost or stolen, the encrypted data remains secure even if the repository is attached to a system modified to bypass normal safeguards.

KUNZLER & ASSOCIATES
ATTORNEYS AT LAW
8 EAST BROADWAY, SUITE 600
SALT LAKE CITY, UTAH 84111